Threat Bulletin: Weaponized Software Targets Chinese-Speaking Organizations

1/17/2025

Written by Nicole Fishbein - 16 January 2025

Top Blogs

Overview of the Attack

Intezer Labs research team has identified a series of attacks targeting organizations in Chinese-speaking regions like Hong Kong, Taiwan, and China itself. These attacks utilize a multi-stage loader, which we named **PNGPlug**, to deliver the **ValleyRAT** payload.

A similar attack chain is documented in this report, which sheds light on the infection vector and the method of delivering the malicious files.

According to the report, the attack begins with a phishing webpage designed to encourage victims to download a malicious MSI (Microsoft Installer) package disguised as legitimate software.

Upon execution, the installer performs two critical tasks:

1. Deploying a benign application to maintain the illusion of legitimacy.
2. Extracting an encrypted archive containing the malware payload.

The MSI package uses the Windows Installer's *CustomAction* feature, enabling it to execute malicious code, including running an embedded malicious DLL that decrypts the archive (`all.zip`) using a hardcoded password `hello202411` to extract the core malware components:

- **`libcef.dll`**: The loader, designed with padding to inflate its size to 220MB, helps it evade detection as many security tools skip analyzing large files. (For more information about how this technique is used in loaders, check out our recent blog post.)
- **`down.exe`:** A legitimate application used to mask malicious activities.
- **`aut.png` and `view.png`**: Files masquerading as PNG images containing encoded malicious payloads.

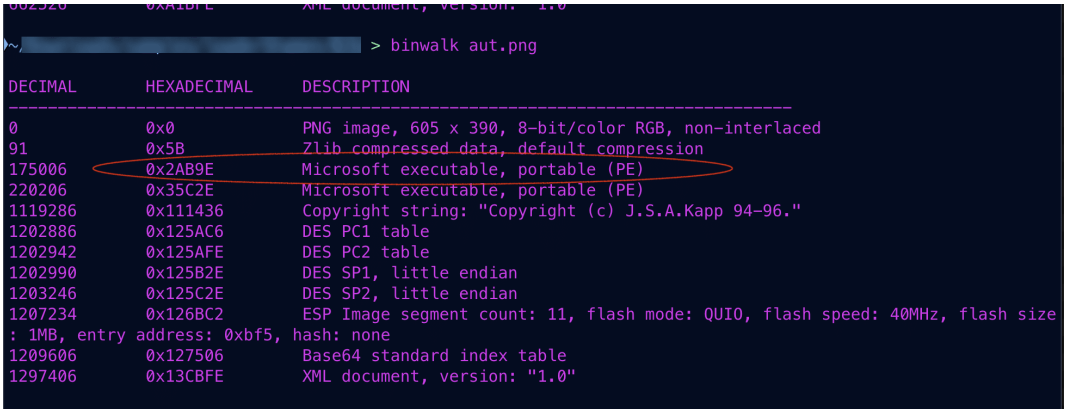
Role of the PNGPlug Loader

The primary function of the loader (`libcef.dll`) is to set up the environment for malware execution via the following steps:

1. **Patching `ntdll.dll`**: Enables memory injection.
2. **Command-line Argument Parsing**:
    - If the `/aut` argument is present, the loader decrypts the registry path `Software\\DICKEXEPATH` using XOR encryption and writes the `down.exe` path to the registry (`HKEY_CURRENT_USER\Software\DICKEXEPATH`). The loader then uses the pe_to_shellcode injection method to inject the contents of `aut.png` into memory. (For more information about this injected payload, refer to this report.)
    - If `/aut` is absent, the loader runs `down.exe` with the argument and continues its checks.

3. **Anti-Virus Detection**: The loader searches for the presence of 360 Total Security by checking the path `C:\Program Files (x86)\360\360Safe\uninst.exe`. If absent, the loader maps `view.png` into memory and creates a new process (`colorcpl.exe`), injecting the contents of `view.png`. During investigations, the process was executing ValleyRAT malware.

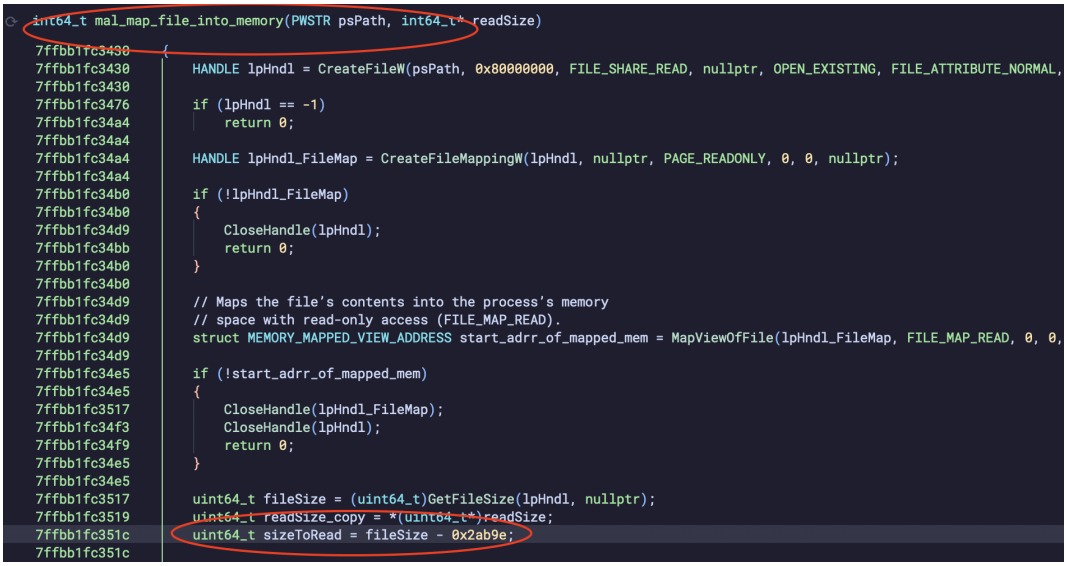
The use of .png file extensions for malicious payloads is a key stealth tactic and inspired the name **PNGPlug**. As shown in the screenshots below, these PNG files contain additional data, specifically PE executables, embedded at specific offsets. This data is loaded and injected into the process as described earlier, further enhancing the malware's ability to evade detection while executing its payload.



```
~/                                    > binwalk aut.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 605 x 390, 8-bit/color RGB, non-interlaced
91            0x5B            Zlib compressed data, default compression
175006        0x2AB9E         Microsoft executable, portable (PE)
220206        0x35C2E         Microsoft executable, portable (PE)
1119286       0x111436        Copyright string: "Copyright (c) J.S.A.Kapp 94-96."
1202886       0x125AC6        DES PC1 table
1202942       0x125AFE        DES PC2 table
1202990       0x125B2E        DES SP1, little endian
1203246       0x125C2E        DES SP2, little endian
1207234       0x126BC2        ESP Image segment count: 11, flash mode: QUIO, flash speed: 40MHz, flash size
: 1MB, entry address: 0xbf5, hash: none
1209606       0x127506        Base64 standard index table
1297406       0x13CBFE        XML document, version: "1.0"
```

Binwalk output for one of the PNG files used by the loader, demonstrating that it has a Windows executable (PE) at offset 0x2AB9E.



```
int64_t mal_map_file_into_memory(PWSTR psPath, int64_t* readSize)
{
    HANDLE lpHndl = CreateFileW(psPath, 0x80000000, FILE_SHARE_READ, nullptr, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL,

    if (lpHndl == -1)
        return 0;

    HANDLE lpHndl_FileMap = CreateFileMappingW(lpHndl, nullptr, PAGE_READONLY, 0, 0, nullptr);

    if (!lpHndl_FileMap)
    {
        CloseHandle(lpHndl);
        return 0;
    }

    // Maps the file's contents into the process's memory
    // space with read-only access (FILE_MAP_READ).
    struct MEMORY_MAPPED_VIEW_ADDRESS start_adrr_of_mapped_mem = MapViewOfFile(lpHndl_FileMap, FILE_MAP_READ, 0, 0,

    if (!start_adrr_of_mapped_mem)
    {
        CloseHandle(lpHndl_FileMap);
        CloseHandle(lpHndl);
        return 0;
    }

    uint64_t fileSize = (uint64_t)GetFileSize(lpHndl, nullptr);
    uint64_t readSize_copy = *(uint64_t*)readSize;
    uint64_t sizeToRead = fileSize - 0x2ab9e;
```

A function in the loader that handles the mapping of the PNG file into the memory. Specifically, it looks for the data that begins at offset

ValleyRAT Details

ValleyRAT is a sophisticated, multi-stage malware attributed to the **Silver Fox APT**. It employs advanced techniques such as:

- **Shellcode Execution**: Running components directly in memory to reduce its file footprint and evade detection.
- **Obfuscation and Privilege Escalation**: Hiding malicious activities and gaining elevated access.
- **Persistence Mechanisms**: Leveraging scheduled tasks and registry modifications to maintain control over infected systems.

The malware's stages include initial execution, deployment of obfuscated shellcode, and a loader module that fetches additional malicious components from its command-and-control (C2) server.

Attribution

Evidence links this campaign to the **Silver Fox APT**, a group known for espionage and cybercrime campaigns targeting Chinese-speaking individuals and organizations. Their tactics include:

- **Phishing Techniques**: Using trojanized files and SEO-optimized phishing sites.
- **Espionage Tools**: Deploying malware like ValleyRAT and Gh0st RAT to monitor user activities, deliver plugins, and potentially install additional payloads.

Based on victimology, infection vectors, and observed payloads, we attribute this campaign to Silver Fox with high confidence. Their operations underscore the need for robust cybersecurity measures to counter evolving threats from

sophisticated actors.

What's Interesting?

This campaign stands out due to its unique focus on Chinese-speaking victims and organizations across China, Hong Kong, and Taiwan. It demonstrates an attack that broadly targets one specific demographic—the Chinese-speaking. Interestingly, despite their well-documented disputes and distinct political landscapes, the attackers are treating these regions as a unified target. This differs from the conventional perspective within the security community, which often considers them separately when analyzing threats.

Another notable aspect of these attacks is the potential operational gaps within these organizations, particularly the lack of investment in employee tools among some larger companies. This oversight frequently forces employees to rely on free software, inadvertently increasing their vulnerability to malicious campaigns.

Equally striking is the attackers' sophisticated use of legitimate software as a delivery mechanism for malware, seamlessly blending malicious activities with seemingly benign applications. The adaptability of the PNGPlug loader further elevates the threat, as its modular design allows it to be tailored for multiple campaigns. This flexibility underscores the evolving nature of the threat landscape, emphasizing the urgent need for advanced detection and prevention mechanisms to counter these stealthy and persistent attacks.

IOCs

156.247.33[.]53

- 08dad42da5aba6ef48fca27c783f78f06ab9ea7a933420e4b6b21e12e550dd7d
- 33bc111238a0c6f10f6fe3288b5d4efe246c20efd8d85b4fe88f7d602d70738e
- 50a64e97c6a5417023f3561f33291b448ce830a4d99c40356af67301c8fa7523
- 6d4dd4334791c91bb09e7a91dd5c450b2c6e3348a5586de011c54ce3f473f619
- 76fc76dc651c3cc9d766a6ad8a90f605326463bc4cb2f8f053d44dfbc913beee
- ad23f5c9bab137dc24343fc410f7587885aab6772dee5e75a216ed579c6ee420
- c497506fe2df57c39fcf92398f4864ca4bfcb1a6f2f80c3c520166bc61882855
- E49b085f5484531395b5a7903f004b2a02a2b4ebfa46116d1a665ba881b1f528
- c636120749b49f47fc8d42409ead6c51ea44bc40c815370997ca63f48acdf002
- 79acdca5247ca9719f2f3a34c7942cd60b209f7b616efa5dd81e6656a8baf9a5
- 70facc8ad5db172e235b4cc720a0edaedd4470b8a6ec5da8dee2758f4a1aafef
- e9e4751c88d3a1a4bfdd5d07bb35636787b0d6fbf68b17642d3fe03cbe5ebf70
- de8a0da702a491f610b9e85050d8641cadf4ed84edf4d151f94335b0d78d6636
- 6d2a4d9e2fc6e4dac2c426851b4bdf86dd63a5515d8d853e622a0bc01d250ce9
- 4a68bdfa3e31a8c063bbf94469160eb7998a556027d5ad33f37c347a71c2d3a4
- 7c31c4d0308fb1d67f6af48a76138a9db19f494c1e9a12debdcca7382ad5418c
- 5f9a5ad43a9f79976cd7014ce072429ef2edbae872b4226372cfb07d8a86b8a5
- 3ac3ca18142a935608cb0d2c8d6421ebb9abc30bce93f094447b9c3f63fe791b
- 9d97f3f55bc647911e14a36c83f263e91662cf9d13a2fc3ec7c92dedb8977d37
- c070749f95aeeefcd1c3a875c1b8e77b57cad0c8338436af9a3c9e1323fd4e11
- 7eaed6fa867875119c3ebb40aa24716d91fdbccb2106fa4708ff0637920a920c
- fa26722e99763a29af160fae64183a47a57362b666753624b78e954c8cde0525
- 9aa51d1c82fdbc8f0f27340180bd40faa7e76b8ac6d204b2d3548cfd0897d805
- 58416315c61ed5cb2c754244ed5c081963dabf3e698b04226a00f978cd913e84
- f2f96e5ac1b4bd6cac49c71ca2010dcbe5751757483520cfc7dddf4fb7186044

45.195.148[.]107

- 46af73560cafff5c8bbc16980d01641af0de3b689bc248dfb52afcf3a8a76a55
- 7bff2404c2816c4e1576d449820f01e3f46e7c972beb1843e3b8da2e065f8dc3
- 94ff4679dd5aec7874354c14132701ecdfbbb558c6011e4952d13bf843255529
- Ae6d88ea99e530f778ee6088862b50dfb6e8bb45857211e9105428c57c2a7b4a
- *9aea0fdfead2e956bc0b4574c2b4cb2855dd9df6a5fd61d350f3285d249adfca*

First stage of the loader:

- c5d5054047a12efc68a67abd8f15069a853dd09800cd39d68df5a27702b45334
- a97371df7d51fe0aee1d54b5b233a1713f69224802b1da35337a3041788990e6
- 4b6bf40dc331c89e416ef012a6dc4f55c83136197be7115246b42e4f7a828baa
- 30147b6691e5bc1a15c76cebf81b2de77d9099e8200b6ed9742c6e3b36505f34
- 9bd53057c8905d508374698e2595301f0be1529ec4ebfa71c09ad0c01a562982
- 4d64c2d1ae0de0f3066a6c020ab7aa5a9dd487c0cf1ff1ca2e93d98ff30e039f
- 99fb7a40dbf6a042bcb77f67a5a76fe03ec3c6820ac5e15cb009795d545152ea
- d9e939f904a1cddf5fb8ffba14acbfe227ed5dfc4990b52a44d4dfd0baa6de4e
- 0b33f08bc2917c4825c053754fc88e16b35d1a8fff4135595b265a4c6f850250
- cd347b9f558cf024df1dbb62ed7a0d72a2edc04b1330058cfa1baf4fc3894e03

- 8aa28f35dbafc18a37b07fd15bb599e3c8de5b692117f1c6fd491bd03028a423
- d51db234d0236cd0dbfcf13adc33387f10920011537815d188eff012872e30be
- d0ce85ec31053478c67e4f53ca2ef9b7b1f0fda74621c9c7c8c1612772ca778c
- 504d7714419931f80b734e212a9431ec98887c56ade8966c4d7cae58b28d49ca
- 16bb3968e1112b63fef8a4e7bda9d021dfef6fd1955fdfa677545535a14a65b4
- 659ede632d3bfc28d143c144fdba34d08b21c4f97ce6c9dc1fcd4d2bf5cc25e3
- 463c9704fb009cd13e0ef50fa7d5035aa5f35b4841fe75ecab5c4a276601f837
- 3fc35cab1272f769af309cb46375e21680f13d629181c7646cb0cf2c9b2e72e7
- 517b43bf057877727387316d8538dc07599856eb428d43f512e89964a5dfb331
- e54ce9939679c691dc5719e309a8d541183b6672269fd61013109ef0d8509b1e